REMARKS

This paper is responsive to a non-final Office action dated December 30, 2008. Claims 1-3, 5-16, 18-22, 26-32, 41-43, 45-47, and 57 were examined.

Claim Rejections Under 35 U.S.C. § 103 Over Medvinsky and Jung

Claims 1-3, 5-8, 14-16, 18-22, 26, 27, 41-43, and 45-47 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky in view of U. S. Patent Application Publication No. 2001/0052072 to Jung (hereinafter, "Jung").

Regarding claim 14, Applicants respectfully maintain that Medvinsky, alone or in combination with Jung, fails to teach or suggest

> padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet,

as required by claim 14. Applicants respectfully point out that those limitations of the method of generating an encrypted data packet of claim 14 require both padding data and de-padding padded, encrypted data to form the encrypted payload.

Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free

> running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet, as required by claim 14.

Jung fails to compensate for the shortcomings of Medvinsky. Jung teaches that

> [t]he encryption/decryption module 24 is primarily responsible for encrypting the outgoing speech data packets and decrypting the incoming speech data packets. In one embodiment, a stream encryption algorithm is used by the encryption/decryption module 24 to encrypt and decrypt the data packets. Note, however, that the specific type of stream encryption algorithm used is not important to the invention, and that any known or yet to be developed stream encryption may be used without departing from the scope of the invention. The tasks performed by the encryption/decryption module 24 include such things as performing certain mathematical/logical operations on the data (depending on the type of encryption used), padding the data where applicable, and other tasks related to the encryption/decryption process.

Paragraph 0035 (emphasis added). The system of Jung includes an encryption/decryption module that pads the data where applicable. Paragraph 0035. Padding data where applicable, as taught by Jung fails to teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the

fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet, as required by claim 14. No other portion of Jung teaches those limitations of claim 14.

Applicants respectfully point out that in determining whether the subject matter of a patent claim is obvious, "[w]hat matters is the objective reach of the claim." KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 16; 82 USPQ2d 1385, 1397 (U.S. 2007). "If the claim extends to what is obvious, it is invalid under § 103." See id. To be nonobvious, an improvement must be "more than a predictable use of prior art elements according to their established functions." See id. at 13; 1396. Applicants maintain that the differences between the claim and the prior art are not predictable uses of prior art elements according to their established functions and the Office has failed to satisfy other obviousness inquiries (e.g., simple substitution of one known element for another to obtain predictable results, use of a known technique to improve similar devices in the same way, applying a known technique to a known device ready for improvement to yield predictable results, known work in one field of endeavor prompting variations of it for use in the same field or a different one based on design incentives or other market forces if the variation would have been predictable to one of ordinary skill in the art, or some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the reference or to combine the prior art teachings to arrive at the claimed invention). The Office has failed to establish that it is predictable to both pad data and de-pad padded, encrypted data to form the encrypted payload, as required by claim 14, based on padding data as taught by Jung. Both padding data and de-padding padded, encrypted data to form the encrypted payload, as required by claim 14 is not a predictable result of the requirement of stream encryption algorithms that the transmitter and receiver sides be synchronized, as implied by the Office action. Applicants respectfully maintain that the Office's proposed combination is not a predictable use of the padding taught by Jung.

Thus, the combination of Medvinsky and Jung fails to establish a *prima facie* case of obviousness of the limitations of claim 14. Therefore, independent claim 14 is allowable, as well

as the claims depending therefrom. Accordingly, the rejection of claims 14-16, 18-22, 26, and 27, should be withdrawn.

Regarding claim 41, Applicants respectfully maintain that Medvinsky, alone or in combination with Jung, fails to teach or suggest

> a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload,

as required by claim 41. Applicants respectfully point out that those limitations of claim 41 require a transmitter that includes both a padding engine configured to generate padded data and a pad remover configured to generate the encrypted data packet.

Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key

stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload, as required by claim 41.

Jung fails to compensate for the shortcomings of Medvinsky. Jung teaches that

> [t]he encryption/decryption module 24 is primarily responsible for encrypting the outgoing speech data packets and decrypting the incoming speech data packets. In one embodiment, a stream encryption algorithm is used by the encryption/decryption module 24 to encrypt and decrypt the data packets. Note, however, that the specific type of stream encryption algorithm used is not important to the invention, and that any known or yet to be developed stream encryption may be used without departing from the scope of the invention. The tasks performed by the encryption/decryption module 24 include such things as performing certain mathematical/logical operations on the data (depending on the type of encryption used), padding the data where applicable, and other tasks related to the encryption/decryption process.

Paragraph 0035 (emphasis added). The system of Jung includes an encryption/decryption module that pads the data where applicable. Paragraph 0035. Padding data where applicable, as taught by Jung fails to teach or suggest a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload, as required by claim 41. No other portion of Jung teaches those limitations of claim 41.

Applicants respectfully point out that in determining whether the subject matter of a patent claim is obvious, "[w]hat matters is the objective reach of the claim." KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 16; 82 USPQ2d 1385, 1397 (U.S. 2007). "If the claim extends to what is obvious, it is invalid under § 103." See id. To be nonobvious, an improvement must be "more than a predictable use of prior art elements according to their established functions." See id. at 13; 1396. Applicants maintain that the differences between the

claim and the prior art are not predictable uses of prior art elements according to their established functions and the Office has failed to satisfy other obviousness inquiries (e.g., simple substitution of one known element for another to obtain predictable results, use of a known technique to improve similar devices in the same way, applying a known technique to a known device ready for improvement to yield predictable results, known work in one field of endeavor prompting variations of it for use in the same field or a different one based on design incentives or other market forces if the variation would have been predictable to one of ordinary skill in the art, or some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the reference or to combine the prior art teachings to arrive at the claimed invention). The Office has failed to establish that it is predictable for a transmitter to include both a padding engine configured to generate padded data and a pad remover configured to generate the encrypted data packet, as required by claim 41, based on padding data as taught by Jung. A padding engine configured to generate padded data and a pad remover configured to generate the encrypted data packet, as required by claim 41 is not a predictable result of the requirement of stream encryption algorithms that the transmitter and receiver sides be synchronized, as implied by the Office action. Applicants respectfully maintain that the Office's proposed combination is not a predictable use of the padding taught by Jung.

Thus, the combination of Medvinsky and Jung fails to establish a *prima facie* case of obviousness of the limitations of claim 41. Therefore, independent claim 41 is allowable, as well as the claims depending therefrom. Accordingly, Applicants respectfully request that the rejection of claims 41-43 and 45-47 be withdrawn.

Regarding claim 1, Applicants respectfully maintain that Medvinsky, alone or in combination with Jung, fails to teach or suggest

> padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to

> the encrypted payload, a remaining portion of the fixed length segment being applied to the padding,

as required by claim 1. Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 1.

Jung fails to compensate for the shortcomings of Medvinsky. Jung teaches that

> [t]he encryption/decryption module 24 is primarily responsible for encrypting the outgoing speech data packets and decrypting the incoming speech data packets. In one embodiment, a stream encryption algorithm is used by the encryption/decryption module 24 to encrypt and decrypt the data packets. Note, however, that the specific type of stream encryption algorithm used is not important to the invention, and that any known or yet to be developed stream encryption may be used without departing from the scope of the invention. The tasks performed by the encryption/decryption module 24 include such things as performing certain mathematical/logical operations on the data (depending on the

> type of encryption used), padding the data where applicable, and other tasks related to the encryption/decryption process.

Paragraph 0035 (emphasis added). The system of Jung includes an encryption/decryption module that pads the data where applicable. Paragraph 0035. Padding data where applicable, as taught by Jung fails to teach or suggest padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 1. No other portion of Jung teaches those limitations of claim 1.

Applicants respectfully point out that in determining whether the subject matter of a patent claim is obvious, "[w]hat matters is the objective reach of the claim." KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 16; 82 USPQ2d 1385, 1397 (U.S. 2007). "If the claim extends to what is obvious, it is invalid under § 103." See id. To be nonobvious, an improvement must be "more than a predictable use of prior art elements according to their established functions." See id. at 13; 1396. Applicants maintain that the differences between the claim and the prior art are not predictable uses of prior art elements according to their established functions and the Office has failed to satisfy other obviousness inquiries (e.g., simple substitution of one known element for another to obtain predictable results, use of a known technique to improve similar devices in the same way, applying a known technique to a known device ready for improvement to yield predictable results, known work in one field of endeavor prompting variations of it for use in the same field or a different one based on design incentives or other market forces if the variation would have been predictable to one of ordinary skill in the art, or some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the reference or to combine the prior art teachings to arrive at the claimed invention). The Office has failed to establish that it is predictable to pad an encrypted payload of a received data packet, as required by claim 1, based on padding data as taught by Jung. Padding an encrypted payload of a received data packet, as required by claim 1 is not a predictable result of the requirement of stream encryption algorithms that the transmitter and receiver sides be

synchronized, as implied by the Office action. Applicants respectfully maintain that the Office's proposed combination is not a predictable use of the padding taught by Jung.

Thus, the combination of Medvinsky and Jung fails to establish a *prima facie* case of obviousness of the limitations of claim 1. Therefore, independent claim 1 is allowable, as well as the claims depending therefrom. Accordingly, Applicants respectfully request that the rejection of claims 1-3 and 5-8, be withdrawn.

Claim Rejections Under 35 U.S.C. § 103 Over Medvinsky, Jung, and Staring

Claims 9-13 and 28-32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky in view of Jung, and further in view of U.S. Patent Application Publication No. 2001/0007127 to Staring (hereinafter, "Staring").

Regarding claims 28-32, Applicants respectfully maintain that Medvinsky, alone or in combination with Jung and Staring, fails to teach or suggest

> padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet,

as required by claim 14 from which claims 28-32 indirectly depend. Applicants respectfully point out that those limitations of the method of generating an encrypted data packet of claim 14 require (and the references of record fail to teach or suggest) both padding data and de-padding padded, encrypted data to form the encrypted payload.

As described above with regard to the first ground of rejection, Medvinsky and Jung fail to teach or suggest those limitations of claim 14. Staring fails to compensate for the shortcomings of Medvinsky and Jung. Staring teaches that

> [t]he block cipher is preferably the Digital Encryption Standard (DES) in Cipher Block Chaining (CBC) mode. To preserve data payloads and to minimize data payload overhead, Cipher Text Stealing CTS) is preferably used. The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again. However, this increases the data payload size and in addition, the number of padded bytes must be conveyed to the decrypting side to remove the padding bytes correctly. A better method is to use Cipher Text Stealing.

Paragraph [0049]. The padding of data blocks on the transmit side and removing padding bytes at the receive side of Staring fails to teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet, as required by claim 14.

Staring teaches further a cipher text stealing technique:

> Referring to the example of FIG. 6, the first two plain text blocks P_1 and P_2 are encrypted in the conventional way using a Cipher Block Chaining mode. So, P_2 is combined (XOR-ed) with the ciphertext C_1 of the encryption outcome for the first block and encrypted giving $E_k(P_2 \oplus C_1)= C_2$. The third block P_3 is also encrypted conventionally, giving $E_k(P_3 \oplus C_2)$. In the example, the last plaintext block P4 contains only 2 bytes. This number of bytes is taken from the beginning of the encryption outcome and used as the ciphertext for block 4. This can be represented as: $E_k(P_3 \oplus C_2)=C_4|C'$ (where "|" represents a concatenation). C' is not transmitted. The last block P_4 is padded (in this example six bytes are added), represented by $P_4|PAD$ (for the padding bits any bit value may be used). As normal, this is combined with the previous encryption outcome and encrypted, giving the third ciphertext block $C_3= E_k((P_4|PAD) \oplus (C_4|C'))$. C_3 and C_4 are transmitted. In the receiving system, first C_3 is decrypted, giving $(P_4|PAD) \oplus (C_4|C')$. Next C4 is padded with the same PAD bits. The result is XOR-ed with the decryption result, giving: $(C_4\uparrow PAD) \oplus ((P_4|PAD) \oplus (C_4|C'))=(P_4|C')$. This provides P_4 and C'. Next C_4 is padded with C' and decrypted, giving $P_3 \oplus C_2$. By XOR-ing this with C_2 access is obtained to P_3.

Paragraph [0050]. The cipher text stealing techniques of Staring include padding a payload, encrypting the padded payload, transmitting a resulting ciphertext block, padding a received ciphertext block, and decrypting the received ciphertext block. Col. 9, lines 33-44. The cipher text stealing technique of Staring and other portions of Staring fail to teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet, as required by claim 14.

Since Medvinsky, Jung, and Staring fail to teach or suggest the limitations of claim 14 from which claims 28-32 indirectly depend, Applicants respectfully request that the rejection of claims 28-32 be withdrawn.

Regarding claims 9-13, Applicants respectfully maintain that Medvinsky, alone or in combination with Jung and Staring, fails to teach or suggest

> padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding,

as required by claim 1 from which claims 9-13 indirectly depend. As described above with regard to the first ground of rejection, Medvinsky and Jung fail to teach or suggest those limitations of claim 1. Staring fails to compensate for the shortcomings of Medvinsky and Jung. Staring teaches that

> [t]he block cipher is preferably the Digital Encryption Standard (DES) in Cipher Block Chaining (CBC) mode. To preserve data payloads and to minimize data payload overhead, Cipher Text Stealing CTS) is preferably used. The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again. However, this increases the data payload size and in addition, the number of padded bytes must be conveyed to the decrypting side to remove the padding bytes correctly. A better method is to use Cipher Text Stealing.

Paragraph [0049]. The padding of data blocks on the transmit side and removing padding bytes at the receive side of Staring fails to teach or suggest padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 1.

> Staring teaches further a cipher text stealing technique:
>
> Referring to the example of FIG. 6, the first two plain text blocks P_1 and P_2 are encrypted in the conventional way using a Cipher Block Chaining mode. So, P_2 is combined (XOR-ed) with the ciphertext C_1 of the encryption outcome for the first block and encrypted giving $E_k(P_2 \oplus C_1)= C_2$. The third block P_3 is also encrypted conventionally, giving $E_k(P_3 \oplus C_2)$. In the example, the last plaintext block P4 contains only 2 bytes. This number of bytes is taken from the beginning of the encryption outcome and used as the ciphertext for block 4. This can be represented as: $E_k(P_3 \oplus C_2)=C_4|C'$ (where "|" represents a concatenation). C' is not transmitted. The last block P_4 is padded (in this example six bytes are added), represented by $P_4|PAD$ (for the padding bits any bit value may be used). As normal, this is combined with the previous encryption outcome and encrypted, giving the third ciphertext block $C_3= E_k((P_4|PAD) \oplus (C_4|C'))$. C_3 and C_4 are transmitted. In the receiving system, first C_3 is decrypted, giving $(P_4|PAD) \oplus (C_4|C')$. Next C4 is padded with the same PAD bits. The result is XOR-ed with the decryption result, giving: $(C_4\uparrow PAD) \oplus ((P_4|PAD) \oplus (C_4|C'))=(P_4|C')$. This provides P_4 and C'. Next C_4 is padded with C' and decrypted, giving $P_3 \oplus C_2$. By XOR-ing this with C_2 access is obtained to P_3.

Paragraph [0050]. The cipher text stealing techniques of Staring include padding a payload, encrypting the padded payload, transmitting a resulting ciphertext block, padding a received ciphertext block, and decrypting the received ciphertext block. Col. 9, lines 33-44. The cipher

text stealing technique of Staring and other portions of Staring fail to teach or suggest padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 1.

Since Medvinsky, Jung, and Staring fail to teach or suggest the limitations of claim 1 from which claims 9-13 indirectly depend, Applicants respectfully request that the rejection of claims 9-13 be withdrawn.

Claim Rejections Under 35 U.S.C. § 103 Over Medvinsky and Sengodan

Claim 57 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky and further in view of U.S. Patent No. 6,918,034 to Sengodan et al. (hereinafter, "Sengodan").

Applicants respectfully maintain that Medvinsky, alone or in combination with Sengodan, fails to teach or suggest

> a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine, a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, and a pad remover configured to remove padding from the decrypted data to recover the data,

as required by claim 57. Applicants respectfully point out that those limitations of the receiver of claim 57 require (and the references of record fail to teach or suggest) both a padding engine and a pad remover.

Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine, a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, and a pad remover configured to remove padding from the decrypted data to recover the data, as required by claim 57.

Sengodan fails to compensate for the shortcomings of Medvinsky. Sengodan teaches that "[t]he recipient after decrypting the mini-packet looks at the last byte 524 to determine the number of padding bytes 522 used." Col. 8, lines 19-21. Even though Sengodan teaches a padding technique, that padding technique of Sengodan fails to teach or suggest a receiver that requires both a padding engine and a pad remover, as required by claim 57. Thus, Sengodan fails to teach or suggest a receiver including a padding engine operable to pad an encrypted

payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine, a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, and a pad remover configured to remove padding from the decrypted data to recover the data, as required by claim 57.

Furthermore, Applicants respectfully point out that

> [o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate this review, this analysis should be made explicit.

KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 13; 82 USPQ2d 1385, 1396 (U.S. 2007). Moreover, "'[a] reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference or would be led in a direction divergent from the path that was taken by the applicant.'" In re Kahn, 441 F.3d 977, 990, 78 U.S.P.Q.2d (BNA) 1329, 1338 (Fed. Cir. 2006) (citations omitted). The Office action fails to provide a proper rationale for combining Medvinsky with Sengodan to teach a receiver including both a padding engine and a pad remover, as required by claim 57. Sengodan teaches that "[b]lock encryption schemes require that the packet size be an integral multiple of block size." Col. 3, lines 54-55. Sengodan teaches that mini-packets are padded to "insure each mini-packet is an integral multiple of a predetermined block size." Col. 4, lines 34-36. "The padding added to the data for each packet comprises p-1 units of padding and a final padding unit for indicating the amount of padding" of Sengodan. Col. 4, lines 44-47. The final padding unit is transmitted with the padded mini-packet and received by a receiver of Sengodan. Col. 8, lines 9-21. The receiver of Sengodan that receives the encrypted padded data and an indicator of the amount of padding teaches away from a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the padded encrypted payload of the received encrypted data received by the decryption engine, as required by claim 57.

Thus, the combination of Medvinsky and Sengodan fails to establish a *prima facie* case of obviousness of the limitations of claim 57. Accordingly, Applicants respectfully request that the rejection of claim 57 be withdrawn.

Conclusion

In summary, all claims are believed to be allowable over the art of record, and a Notice of Allowance to that effect is respectfully solicited. Nonetheless, if any issues remain that could be more efficiently handled by telephone, the Examiner is requested to call the undersigned at the number listed below.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

☐ deposited with the US Postal Service with sufficient postage as first class mail in an envelope addressed as shown above.

☐ facsimile transmitted to the USPTO.

☒ transmitted using the USPTO electronic filing system.

/Nicole Teitler Cave/ — Nicole Teitler Cave

03-30-2009 — Date

EXPRESS MAIL LABEL: _____

Respectfully submitted,

/Nicole Teitler Cave/

Nicole Teitler Cave, Reg. No. 54,021
Attorney for Applicant(s)
(512) 338-6315 (direct)
(512) 338-6300 (main)
(512) 338-6301 (fax)